REMARKS/ARGUMENTS

Claims 2-9, 11-14, and 20-28 are pending in the present application.

This Amendment is in response to the Office Action mailed March 24, 2006. In the Office Action, the Examiner rejected claims 2-9, 11-14, and 20-28 under 35 U.S.C. §103(a). Applicant respectfully traverses the rejections in their entirety. Reconsideration in light of the remarks made herein is respectfully requested.

Rejection Under 35 U.S.C. § 103

A. CLAIMS 2-7, 9 AND 12-13

In the Office Action, claims 2-7, 9, 12-13 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,818,939 issued to Davis et al. ("Davis") in view of "Handbook of Applied Cryptography", Section 12.3 ("Menezes") and U.S. Patent No. 6,212,633 issued to Levy et al. ("Levy"). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. See MPEP §2143. At a minimum, Applicant respectfully contends that the combination of Davis, Menezes and Levy does not teach or suggest all of the claim limitations set forth in the above-listed claims.

The Office Action states that Davis discloses a cryptographic unit generating a shared secret key which is allegedly equivalent to the "long-term value" as claimed (Office Action, page 3). Applicant respectfully disagrees.

Davis does not disclose *receiving a first command* from a second device by a first device, the first command being *generated only once upon an initial power-up sequence* by the second device, as recited in claim 3. *Emphasis added.* The shared secret key is contained in the cryptographic unit's non-volatile memory element 610 and is also imprinted into the secret key storage element 420 of the chipset normally during manufacture when both units are powered up

and in communication with each other (Davis, col. 5, lines 25-44). Thus, Davis discloses a shared secret key built into the chipset during manufacture and independent of the cryptographic unit that generates the shared secret key whereas claim 3 recites "receiving a first command from a second device by a first device." Davis does not disclose a first command, let alone a first command that is to be generated only once and upon an initial power up sequence as delineated in claim 3. Moreover, Davis does not disclose "within a first device, *in response to the first command*, generating data" as recited in claim 3. *Emphasis added.* Given that the cryptographic unit in Davis does not receive a first command, the cryptographic unit cannot generate data in response to the first command.

The Office Action further states that the cryptographic unit generates a session key *in response* to a communication session which is a periodic event (Office Action, page 3). *Emphasis added.* Applicant respectfully disagrees. The periodic event is not equivalent to a communication session given that the periodic event is further delineated in claim 3 as being a power up sequence. Moreover, Davis merely discloses "the shared secret key may be used by both chipset 315 and cryptographic unit 355 ... to establish a session key" (Davis, col. 5, lines 25-44). Since Davis does not disclose a periodic event triggers the cryptographic unit to generate the session key, generating the session key was not in response to a periodic event.

Applicant agrees that Davis does not disclose that the cryptographic unit generates the session key by generating the short-term value and combining the long-term shared key with the short-term value (Office Action, page 3). However, Applicant respectfully disagrees with the contention that Menezes discloses the limitation (Office Action, page 3). Menezes merely discloses A and B computing the session key using $h'_K(r_B)$, where (1) A selects and sends r_A to B and (2) B selects and sends r_B and other values to A (Menezes, section 12.20). Menezes does not disclose that B generates the short term value in response to a periodic event since the period at which A sends r_A to B is unknown. In contrast, the short term value in the claimed invention is generated once per power cycle in response to an event such as an initialization of devices (Specification, page 6, lines 25-31).

Finally, Applicant agrees that Davis does not disclose that the periodic event is a power-up sequence (Office Action, page 4). However, the Office Action contends that Levy discloses

that new session keys are generated in response to a power-up sequence (Office Action, page 4). Applicant respectfully disagrees.

Levy merely discloses "an authorization list ... may be dynamically recreated for the node in response to ... power on reset" (Levy, col. 16, lines 54-62). Here, the authorization list is a data structure containing a list of authorized nodes (Levy, col. 9, lines 40-41) whereas the secret value may be a cryptographic key (Specification, page 7, line 21). Moreover, Levy merely discloses "a session key may also be permanently stored or dynamically recreated for any given node" (Levy, col. 16, lines 54-62) or "generated each time the communication interface is reset" (Levy, col. 9, lines 46-59), but not in response to power on reset. Since the communication interface resetting does not affect the entire platform, it differs from the power-up sequence recited in claim 3.

With respect to independent claim 9, Applicant incorporates the arguments set forth above. Claim 9 recites "the long term value generated upon detecting an initial power-up sequence and *receipt of information from a second device*." As above, (1) Davis does not disclose the cryptographic unit generating the shared secret key upon receiving information from another device; (2) Menezes does not disclose the short term value being modified after each periodic event; and (3) Levy does not disclose that new session keys are generated in response to a power-up sequence.

Hence, Applicant respectfully submits that a *prima facie* case of obviousness has not been established and respectfully requests withdrawal of the §103(a) rejection as applied to independent claims 3 and 9 and those claims dependent thereon.

B. CLAIMS 8 AND 14

In the Office Action, claims 8 and 14 were rejected under 35 U.S.C. §103(a) as being unpatentable over Davis in view of Menezes and Levy and further in view of "Handbook of Applied Cryptography", Section 10.2 ("Menezes"). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established. In the Office Action, the Examiner states that Menezes does disclose that the hash operation is performed successively (Office Action, page 7). However, the Examiner rejects the claims based on teachings that were previously identified by the Examiner as being nonexistent and furthermore, cited in a section of

Menezes not provided to date. Based on the allowability of these claims on their merit and their dependency on independent claims 1 and 9, believed by Applicant to be in condition for allowance, no further discussion as to the grounds of traverse are warranted. Applicant reserves the right to present such arguments if an Appeal is warranted. Withdrawal of the §103(a) rejection as applied to claims 8 and 14 is respectfully requested.

C. CLAIM 11

In the Office Action, claim 11 was rejected under 35 U.S.C. §103(a) as being unpatentable over Davis in view of Menezes and Levy as applied to claim 9 above and further in view of "INTEL: Intel introduces new chipset for Intel Pentium III processor-based performance PCs" ("Burns"). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established for this claim.

Applicant agrees that Davis does not disclose an I/O control hub (ICH). However, the Office Action contends that Burns teaches the limitation (Office Action, page 7). Applicant respectfully disagrees.

Burns merely discloses a chipset consisting of an I/O Controller Hub which includes an Alert on LAN feature that allows a non-booting system to send a status update to the network administrator when the microprocessor is not present (Burns, pages 1-2), but does not disclose *transmitting a first command* from I/O control hub to the trusted platform module. *Emphasis added.* The capability to send status updates to a network administrator does not indicate that I/O Controller Hub can send commands or moreover commands such as "GenerateLTV" to a trusted platform (Specification, page 6, lines 3-5).

Withdrawal of the §103(a) rejection as applied to claim 11 is respectfully requested.

D. CLAIMS 20, 22-23, 25-26 AND 28

In the Office Action, claims 20, 22-23, 25-26, and 28 were rejected under 35 U.S.C. §103(a) as being unpatentable over Davis in view of Menezes (Section 12.3). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established for this claim.

With respect to independent claims 20 and 25, Applicant incorporates the arguments set forth above. Claim 20 recites "an asymmetric key generation unit to generate, in response to an initial non-repeating event, a unique long term value ... and to generate, in response to a periodic event, a short term value." As above, (1) Davis does not disclose the cryptographic unit generating the shared secret key in response to the initial non-repeating event, since the cryptographic unit either contains the shared secret key independent to the power-up sequence (Davis, col. 5, line 25-29) or the shared secret key may be produced after manufacture (Davis, lines 35-36); and (2) Menezes does not disclose generating, in response to a periodic event, a short-term value.

Withdrawal of the §103(a) rejections as applied to independent claims 20 & 25 and those claims dependent thereon is respectfully requested.

E. CLAIMS 21 AND 27

In the Office Action, claims 21 and 27 were rejected under 35 U.S.C. §103(a) as being unpatentable over Davis in view of Menezes as applied to claims 20 and 25 above, and further in view of Levy. Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established for this claim.

With respect to dependent claims 21 and 27, Applicant incorporates the arguments set forth above. Claims 21 and 27 recite "the periodic event includes a power-up sequence by a platform employing the device". Applicant agrees that Davis and Menezes do not disclose that the periodic event includes a power-up sequence. However, as above, Levy does not disclose the limitation because new session keys are not generated in response to a power-up sequence.

Withdrawal of the §103(a) rejection as applied to claims 21 and 27 is respectfully requested.

F. CLAIM 24

In the Office Action, claim 24 was rejected under 35 U.S.C. §103(a) as being unpatentable over Davis in view of Menezes as applied to claim 20 above, and further in view of Menezes (Section 10.2). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established for this claim.

As above, in the Office Action, the Examiner states that Menezes does disclose that the hash operation is performed successively (Office Action, page 10). However, the Examiner rejects the claim based on teachings that were previously identified by the Examiner as being nonexistent and furthermore, cited in a section of Menezes not provided to date. Based on the allowability of the claim on its merit and its dependency on independent claim 20, believed by Applicant to be in condition for allowance, no further discussion as to the grounds of traverse are warranted. Applicant reserves the right to present such arguments if an Appeal is warranted. Withdrawal of the §103(a) rejection as applied to claim 24 is respectfully requested.

Therefore, Applicant believes that independent claims 3, 9, 20, and 25 and their respective dependent claims are distinguishable over the cited prior art references. Accordingly, Applicant respectfully requests the rejections under 35 U.S.C. §103(a) be withdrawn.

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: June 22, 2006

By _____
William W. Schaal
Reg. No. 39,018
Tel.: (714) 557-3800 (Pacific Coast)

12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☐ *deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.*

Date: June 22, 2006

FACSIMILE

☒ *transmitted by facsimile to the United States Patent and Trademark Office.*

June 22, 2006

Tu Nguyen *Date*